MATIÈRES

19.1 **Objet**

19.2 **Références**

19.3 **Généralités**

19.1 OBJET

19.1.1 Le présent chapitre porte sur le Règlement d'application du règlement sur le traitement d'informations pour la coopération policière internationale.

19.2 RÉFÉRENCES

19.2.1 Règlement adopté par la résolution AG-2007-RES-09 lors de la 76ème session de l'Assemblée générale à Marrakech (Maroc, 2007), entrant en vigueur le 1er janvier 2008.

19.2.2 Règlement amendé par la résolution AG-2008-RES-14 lors de la 77ème session de l'Assemblée générale à Saint-Pétersbourg (Russie, 2008) : introduction des articles 36 à 38, (entrée en vigueur le 1er janvier 2009) ; amendement des articles 18 à 22 et introduction des articles 39 et 40 (entrée en vigueur le 1er septembre 2009).

19.3 GÉNÉRALITÉS

19.3.1 Ce texte porte sur la mise en œuvre des principes de coopération policière et de protection des données énoncés au Règlement sur le traitement d'informations pour la coopération policière internationale, telle que prévue à l'article 23 (c) dudit Règlement.

Le Secrétaire Général

PRÉAMBULE

Rappelant qu'en 2005, lors de sa 74ème session (Berlin, Allemagne), l'Assemblée générale a adopté le projet d'amendement du Règlement sur le traitement d'informations (RTI), qui est entré en vigueur le 1er janvier 2006,

Considérant l'article 2 du RTI qui dispose que ledit règlement fixe les conditions et les principales modalités suivant lesquelles les informations sont traitées par l'Organisation ou par son canal pour les besoins de la coopération policière internationale, dans le respect des droits fondamentaux des individus, conformément à l'article 2 du Statut de l'Organisation et à la Déclaration universelle des droits de l'homme,

Considérant l'article 23 (c) du RTI, qui donne la liste des règles d'application qui devront être approuvées par l'Assemblée générale, pour déterminer les modalités de mise en œuvre, d'une part, des principes de coopération policière et de protection des données énoncés au RTI, et d'autre part, des modalités particulières et/ou procédurales de traitement d'informations ainsi que la manière et les diverses méthodes suivant lesquelles les informations sont enregistrées,

Rappelant que lors de l'adoption du projet d'amendement du RTI en 2005, l'Assemblée générale a demandé au groupe de travail qu'elle a créé en 2002 (71ème session, Cameroun) pour élaborer les règles sur le traitement d'informations, et qu'elle a reconduit tous les ans depuis, de finaliser le projet de règles d'application du RTI au regard des amendements apportés en 2005 audit RTI,

L'Assemblée générale a adopté, lors de sa 76ème session qui s'est tenue à Marrakech (Maroc) du 5 au 8 novembre 2007, le Règlement suivant.

CHAPITRE I

LA RESPONSABILITÉ DES DIFFÉRENTS ACTEURS

Article 1 : Disposition générale

Les dispositions du RTI sur la responsabilité du Secrétariat général, des Bureaux centraux nationaux et des entités autorisées au sens des articles 1 (e), 1 (f) et 1 (g) du RTI sont précisées comme suit.

Article 2 : La responsabilité du Secrétariat général

a) Le Secrétariat général s'assure du respect des règles d'INTERPOL concernant le traitement des informations de police dans les fichiers de l'Organisation. À ce titre, conformément aux dispositions du RTI et notamment de ses articles 4.1 (a,2) et 23 (a), il lui appartient d'entreprendre toute mesure appropriée afin de permettre la mise en œuvre et le respect des dispositions du présent règlement et des textes auxquels il renvoie.

b) Le Secrétariat général doit élaborer les procédures de nature à garantir le respect des règles applicables au traitement de l'information de police, telles que visées au présent règlement et aux textes auxquels il renvoie.

Article 3 : La responsabilité des Bureaux centraux nationaux et des entités autorisées

a) Avant d'autoriser une entité ou un utilisateur désigné à accéder au système d'information d'INTERPOL, l'autorité qui octroie cette autorisation doit s'assurer qu'un tel accès est effectué à des fins de coopération policière internationale.

b) Afin de permettre aux entités sources d'une information d'exercer éventuellement leur droit de restriction, au sens de l'article 5.4 (a) du RTI, les Bureaux centraux nationaux doivent indiquer à quelle(s) base(s) de données et à quelle(s) information(s) ils autorisent les entités visées à l'article 1 (f) à accéder.

c) Les Bureaux centraux nationaux doivent informer les utilisateurs et entités désignés qu'ils autorisent à communiquer des informations par le système d'information policière, de toute nouvelle entité susceptible d'accéder à leurs informations par ledit système.

d) Les entités internationales autorisées doivent également informer les utilisateurs désignés qu'elles autorisent à communiquer des informations par le système d'information policière, de toute nouvelle entité susceptible d'accéder à leurs informations par ledit système.

e) Les Bureaux centraux nationaux, conformément à l'article 5.2 du RTI, et les entités internationales autorisées, sont tenus d'entreprendre toute mesure appropriée pour que les utilisateurs du système d'information policière qu'ils désignent respectent les dispositions du présent règlement et des textes auxquels il renvoie.

f) Les Bureaux centraux nationaux et les entités internationales autorisées devront notamment :

1. mettre en œuvre tout moyen approprié pour que les utilisateurs désignés ou les services nationaux autorisés connaissent et puissent respecter les dispositions du présent règlement et des textes auxquels il renvoie, et qu'à cette fin, ils reçoivent la formation appropriée,

2. retransmettre aux utilisateurs désignés et aux services nationaux autorisés les informations communiquées par le Secrétariat général en vertu de l'article 5.4 (b,1) du RTI,

3. dans la mesure du possible, procéder ou faire procéder à des contrôles du respect du présent règlement et des textes auxquels il renvoie.

g) Les règles de responsabilité applicables aux entités internationales autorisées seront définies dans l'accord de coopération conclu par l'Organisation avec elles, conformément au RTI, au présent Règlement d'application ainsi qu'à toutes autres dispositions générales approuvées par l'Assemblée générale.

h) Les Bureaux centraux nationaux et les entités internationales autorisées informent le Secrétariat général de tout problème lié à l'utilisation ou à la mise en œuvre du système d'information policière, ou encore au respect des règles applicables. Lorsqu'un service national autorisé a connaissance d'un tel problème, il en informe le Bureau central national de son pays.

Article 4 : La responsabilité des utilisateurs

Les utilisateurs doivent :

a) Fournir, dans les meilleurs délais, les informations supplémentaires requises par le Secrétariat général, conformément à l'article 10.1 (c) du RTI, pour lui permettre d'évaluer la possibilité de traiter une information dans les fichiers d'INTERPOL ou la conformité du traitement aux règles applicables, étant entendu que les services nationaux autorisés y procèdent dans les limites déterminées par leurs Bureaux centraux nationaux.

b) S'interdire, conformément à l'article 17.1 (f) du RTI, de recourir à INTERPOL pour communiquer une information ou demander son maintien dans les fichiers de l'Organisation, si ladite information ne peut plus figurer dans leurs propres fichiers.

c) S'assurer, auprès du Secrétariat général et de la source de ladite information, avant toute utilisation d'une information obtenue par le canal d'INTERPOL et via les Bureaux centraux nationaux pour les entités nationales autorisées, que ladite information est toujours d'actualité, exacte, pertinente, et qu'il n'existe pas de restriction à sa retransmission, conformément à l'article 5.5 du RTI. Cette disposition s'applique aussi bien en cas d'accès direct qu'en cas d'accès indirect à une information.

d) En cas de résultat positif obtenu suite à une requête, être en mesure d'informer immédiatement le Bureau central national de leur pays de la raison de la requête, afin que celui-ci puisse répondre aux éventuelles questions posées par la source de l'information suite au message d'alerte généré auprès de ladite source par le résultat positif obtenu.

CHAPITRE II

LES MODALITÉS GÉNÉRALES DE TRAITEMENT D'INFORMATIONS

Article 5 : Disposition générale

Les dispositions du RTI sur les modalités de traitement des informations sont précisées comme suit, conformément aux dispositions des articles 23 (c,2) et 23 (c,4) dudit RTI.

Article 6 : Les différentes catégories de bases de données

Les dispositions de l'article 6 du RTI sont précisées comme suit, conformément aux dispositions dudit RTI, notamment de ses articles 6.2 (e), 10.1 (e) et 10.4 (b).

6.1 - Les bases de données policières

a) Par bases de données policières, on entend toute base créée pour traiter des informations visant à servir des finalités stratégiques ou opérationnelles telles qu'elles sont définies dans l'article 3.1 du RTI.

b) S'il s'avère nécessaire de créer des conditions et modalités de traitement propres à chaque catégorie de base de données, il appartiendra au Secrétariat général d'y procéder, dans le respect du Statut et des règles applicables de l'Organisation. Lorsque ces conditions et modalités spécifiques ont des conséquences pour les B.C.N. ou pour les entités internationales autorisées, ceux-ci doivent en être informés et être consultés.

6.2 - Les bases de données de gestion de la conformité

a) Par bases de données de gestion de la conformité, on entend toute base créée dans le but d'assurer que les informations enregistrées dans les bases de données policières sont conformes au RTI et aux textes auxquels il renvoie, comme il est mentionné dans l'article 6.1 (a) dudit RTI.

b) Ces bases de données ne doivent contenir que les éléments d'information nécessaires pour éviter tout traitement non autorisé ou erroné, visé à l'article 16.2, alinéa (a, 2), du RTI.

c) L'accès à ces bases de données est limité à des services et/ou à des membres du personnel désignés du Secrétariat général participant au traitement de l'information et titulaires d'une autorisation d'accès spécifique.

d) Les éléments d'information traités dans ces bases de données peuvent être conservés pendant 20 ans si cela s'avère nécessaire eu égard à la raison pour laquelle ces éléments sont traités. Cette règle s'applique au traitement manuel et informatique des éléments d'information concernés.

6.3 - Les fichiers d'analyse

a) Les fichiers d'analyse peuvent être reliés ou non au système d'index visé à l'article 6.1 (d) du RTI, suivant la finalité des fichiers en question et les conditions de sécurité et de confidentialité requises.

b) Les informations utilisées dans un fichier d'analyse peuvent être traitées dans les autres bases de données de l'Organisation si elles remplissent les conditions requises à cet effet, sous réserve des restrictions éventuellement imposées par leurs sources.

c) Si les informations traitées dans un fichier d'analyse sont susceptibles de mettre à jour les autres bases de données de l'Organisation, le Secrétariat général doit entreprendre toute mesure appropriée à cette fin.

d) Les rapports d'analyse criminelle doivent :

1. distinguer clairement les informations obtenues du Secrétariat général des conclusions qu'il en a tirées,
2. indiquer la source des informations citées, le statut (au sens de l'article 11 ci-dessous) des personnes et des entités mentionnées et la date à laquelle l'analyse a été réalisée,
3. préciser qu'avant tout usage de ces rapports et des informations qu'ils contiennent, il convient de vérifier, auprès du Secrétariat général et des sources des informations, les droits et restrictions qui y sont attachés.

e) Lorsqu'un projet d'analyse criminelle est achevé :

1. les fichiers d'analyse concernés doivent être détruits,
2. le rapport d'analyse criminelle peut être conservé à condition d'empêcher toute utilisation non pertinente ou contraire aux règles de traitement spécifiées dans le présent règlement et dans tout document auquel il renvoie.

f) La divulgation du rapport d'analyse criminelle ou d'éléments d'informations qui le composent doit respecter les éventuelles restrictions attachées par leurs sources aux informations qu'il contient, ainsi que toute autre mesure de sécurité ou de confidentialité qui lui serait attachée.

Article 7 : Les informations strictement nécessaires à l'identification d'une personne

a) Conformément à l'article 16.2 (a,1) du RTI, les éléments d'information considérés comme strictement nécessaires à l'identification d'un criminel ou d'une personne susceptible de l'être dont le fichier a été détruit, sont notamment les suivants : son nom et son prénom, le numéro de son document d'identité et la nature dudit document, sa date et son lieu de naissance, ainsi que ses empreintes digitales et génétiques, sous réserve des éventuels refus imposés par les sources d'information concernées.

b) Afin de permettre à l'entité demanderesse d'évaluer l'opportunité de s'adresser à la source de l'information, seront également indiqués le nom de ladite source et la référence du message ayant permis d'identifier la source.

c) Ces informations peuvent être conservées pendant dix ans. Elles peuvent être conservées pendant dix années supplémentaires au maximum si cela s'avère nécessaire par rapport à la finalité recherchée. Cette règle s'applique au traitement manuel ou informatique de ces informations.

d) Cependant, ces informations doivent être détruites lorsque la personne qu'elles concernent a été mise hors de cause par une décision de justice. Les sources des informations sont donc tenues d'informer le Secrétariat général dès que ladite personne a été mise hors de cause pour les faits pour lesquels son nom figurait dans les fichiers d'INTERPOL.

e) Le Secrétariat général devra attirer l'attention des utilisateurs sur le fait que ces informations ne sont destinées qu'à orienter le demandeur vers leur source d'origine dans les fichiers d'INTERPOL.

f) Le Secrétariat général élabore les règles de sécurité nécessaires concernant l'accès à ces informations.

Article 8 : L'intérêt concret d'une information pour la police au niveau international

a) Aux fins de l'interprétation et de l'application de la notion d'« intérêt concret pour la police au niveau international », tel que défini à l'article 1 (k) du RTI, il convient d'observer les dispositions ci-dessous.

b) L'intérêt concret pour la police au niveau international d'utiliser le système d'informations d'INTERPOL pour échanger des informations est apprécié par l'utilisateur dudit système et s'effectue sous sa responsabilité.

c) Toute entité qui procède au traitement d'une information évalue son intérêt concret pour la police au niveau international au moment de son enregistrement, de sa mise à jour, de l'évaluation de la nécessité de la conserver dans les fichiers d'INTERPOL, de son utilisation ou encore de sa retransmission, dans la limite des droits dont ladite entité dispose. Cette évaluation s'effectue au regard de :

1. la motivation de la source de l'information,
2. la clarté et la suffisance de l'information,
3. la pertinence et la proportionnalité du traitement de l'information au regard de sa finalité,
4. les risques liés à sa divulgation, notamment au vu des restrictions dont elle peut faire l'objet.

d) Conformément à l'article 10.1(c) du RTI, le Secrétariat général demande à la source de l'information toute précision qu'il juge nécessaire pour lui permettre d'évaluer l'intérêt concret de ladite information pour la police au niveau international et la pertinence de son traitement dans les fichiers d'INTERPOL.

Article 9 : Les dossiers en attente d'informations complémentaires

a) En cas de doute sur la possibilité de traiter une information dans les fichiers d'INTERPOL, au sens de l'article 10.1 (c) du RTI, le Secrétariat général peut enregistrer ladite information pour une durée initiale de six mois, en vue d'obtenir des précisions de la source de l'information ou de l'entité internationale autorisée concernée par ces données. Cette durée peut éventuellement être renouvelée si cela s'avère nécessaire au vu des précisions obtenues.

b) Parallèlement, le Secrétariat général consulte à cette fin la source de l'information ou l'entité internationale autorisée concernée par ladite information.

c) Le Secrétariat général détermine la base de données dans laquelle ces informations peuvent être traitées et l'étendue des droits d'accès qu'il est opportun d'attacher aux dites informations, au regard des doutes liés à leur conformité avec les règles de traitement applicables.

d) Le Secrétariat général indique que l'information n'est pas confirmée ou qu'elle est susceptible de ne pas remplir tous les critères requis pour son traitement, de façon à alerter toutes les personnes susceptibles d'accéder à ladite information, et oriente toute entité demanderesse vers la source de l'information.

Article 10 : Les informations particulièrement sensibles

a) Conformément aux dispositions des articles 10.2 et 17.1 (b) du RTI, les informations particulièrement sensibles ne doivent en aucun cas être traitées, sous quelque forme que ce soit, dans un but discriminatoire ou non conforme aux buts de l'Organisation, tels que définis à l'article 3.1 (a) du RTI.

b) Ces informations sont enregistrées de manière à ce que les utilisateurs puissent les identifier en tant que telles et les traiter conformément aux dispositions du présent règlement et des textes auxquels il renvoie.

c) Elles devront également faire l'objet de contrôles réguliers spécifiques.

Article 11 : Le statut des personnes et les actions requises

a) Le statut d'une personne, au sens de l'article 11 (a, 3, iii) du RTI, définit sa qualité (telle que fugitif, disparu, suspect, témoin, victime, etc.) dans le cadre d'une affaire. Il est déterminé par la source de l'information, ou lorsqu'il y a lieu, par le Secrétariat général au regard des informations dont il dispose soit lorsque les informations ont été enregistrées de sa propre initiative, soit en cas d'omission de la part de la source de ladite information.

b) Au statut d'une personne, doit toujours être attachée l'action à entreprendre envers ladite personne (telle que arrêter, localiser, identifier, etc.).

c) Lors de toute opération de traitement d'une information sur une personne, son statut et l'action à entreprendre envers ladite personne doivent être soigneusement déterminés et systématiquement indiqués.

Article 12 : Les victimes et les témoins

a) Lors de tout traitement d'une information sur une victime ou un témoin, il convient d'indiquer qu'aucune mesure de contrainte ne doit être prise à leur encontre.

b) La notion de témoin s'entend au sens large de spectateur d'une infraction, et peut également comprendre les membres de la famille, voire les amis, les accompagnateurs, les contacts ou les associés d'un suspect ou d'un criminel pour lequel un dossier a été ouvert dans les fichiers d'INTERPOL en vue de le localiser et de l'arrêter.

Article 13 : Les personnes décédées

Un dossier peut être ouvert ou conservé dans les fichiers d'INTERPOL alors que la personne qui en fait l'objet est décédée :

a) en vue de l'identifier,

b) si elle a joué un rôle important dans une affaire traitée dans les fichiers d'INTERPOL et que les informations la concernant sont indispensables à la compréhension de ladite affaire,

c) ou si les informations la concernant peuvent permettre à INTERPOL d'identifier des réseaux, organisations ou associations criminels.

Article 14 : Les personnes morales

Les conditions de traitement d'une information sur une personne physique s'appliquent également aux personnes morales.

Article 15 : La couverture d'événements contextuels spécifiques

Lorsqu'une information est traitée dans les fichiers d'INTERPOL pour couvrir un événement contextuel spécifique, en l'absence d'éléments supplémentaires pouvant justifier sa conservation, elle doit être détruite des fichiers lorsque ledit événement est passé, à moins qu'elle ne puisse être conservée en vertu des articles 14 et 16.2 du RTI, ainsi que de l'article 17 ci-après.

Article 16 : La mise à jour et la destruction des informations liées

a) Lorsque le Secrétariat général met à jour ou détruit une information, soit lorsque cela est nécessaire en vertu du RTI, soit à la demande de sa source, il évalue l'opportunité de mettre à jour ou de détruire le(s) dossier(s) personnel(s) et la ou les affaires auxquelles elle est rattachée.

b) En cas de doute, il consulte le Bureau central national ou l'entité internationale autorisée concernée par l'information en question, conformément à l'article 10.1 (c) du RTI.

c) En cas de destruction d'une information principale, le Secrétariat général détruit aussi les informations subsidiaires ou accessoires qui lui seraient liées, sauf si ces dernières constituent également une information principale en tant que telle ou sont liées à d'autres informations principales. Dans ce cas, l'information ne peut être conservée qu'en rapport avec cette autre affaire et le lien entre les deux affaires doit être détruit.

Article 17 : Le report de la date limite d'évaluation de la nécessité de conserver une information

a) Conformément aux dispositions de l'article 14 (c,2) du RTI, le Secrétariat général peut reporter de sa propre initiative la date limite d'évaluation de la nécessité de conserver une information si les conditions cumulatives suivantes sont remplies :

1. l'information répond toujours aux critères de traitement d'informations dont s'est dotée l'Organisation, et notamment présente toujours un intérêt concret pour la police au niveau international,
2. l'information concerne une infraction majeure ou une forme de criminalité aggravée portant atteinte aux personnes et/ou biens, tels le terrorisme, la criminalité organisée (trafic, réseau), la pédophilie, la récidive, la criminalité en série, ou bien ladite information est liée à une autre affaire dont la mise à jour est toujours assurée par sa source.

b) Quand le Secrétariat général reporte de sa propre initiative la date limite d'évaluation de la nécessité de conserver une information, il entreprend rapidement les démarches appropriées auprès de tout Bureau central national ou toute entité internationale autorisée susceptible d'apporter tout élément pouvant permettre au Secrétariat général de préciser l'information, de la mettre à jour et de continuer à évaluer sa pertinence et son intérêt concret pour la police au niveau international.

CHAPITRE III

LA SÉCURITÉ ET LA CONFIDENTIALITÉ

Article 18 : Disposition générale

Les dispositions des articles du RTI portant sur la sécurité et la confidentialité, visées notamment en ses articles 8 et 9 sont précisées comme suit, conformément aux dispositions de l'article 23 (c,1) dudit RTI.

Article 19 : La sécurité

a) Le Secrétariat général est chargé, en ce qui concerne le système d'information policière de l'Organisation dans son ensemble, y compris les systèmes, réseaux et/ou bases de données spécifiques si nécessaire :

   i. de définir, à partir de normes acceptées au niveau international et en collaboration avec les Bureaux centraux nationaux, une politique en matière de sécurité établissant des dispositifs de sécurité procéduraux, techniques et administratifs à même de garantir des niveaux appropriés de confidentialité, d'intégrité et de disponibilité pour ces systèmes, réseaux et bases de données ;

   ii. de procéder à l'évaluation des risques nécessaire ;

   iii. de mettre en place les dispositifs de contrôle qui conviennent pour que la sécurité des informations soit assurée.

b) Il appartient aux Bureaux centraux nationaux et aux entités internationales autorisées :

   i. d'adopter un niveau de sécurité approprié qui soit au moins équivalent au niveau minimum fixé par les politiques en la matière instaurées par le Secrétariat général ;

   ii. de désigner un ou plusieurs officiers de sécurité chargés des opérations de sécurité pour leur pays ou organisation internationale, qui seront responsables vis-à-vis de leur Bureau central national ou entité internationale autorisée, et assureront la coordination avec le Secrétariat général, suivant nécessité, pour ce qui est des questions de sécurité.

Article 20 : Classification

Aux fins de l'application de l'article 8 du RTI, qui concerne la confidentialité des informations, le présent Règlement d'application définit les différents niveaux de confidentialité des informations ainsi que les conditions attachées à chacun d'entre eux.

Article 20.1 : Niveaux de confidentialité

a) Il existe trois niveaux de confidentialité, correspondant aux risques croissants liés à la divulgation non autorisée des informations :

   1. « À USAGE OFFICIEL INTERPOL UNIQUEMENT »
   2. « DIFFUSION RESTREINTE INTERPOL »
   3. « CONFIDENTIEL INTERPOL »

b) Ces trois niveaux de confidentialité permettent de classifier les informations traitées par le canal d'INTERPOL conformément à l'article 2 du RTI.

   1. Ces niveaux de confidentialité sont utilisés par les Bureaux centraux nationaux, les services nationaux autorisés et les entités internationales autorisées afin d'indiquer aux autres Bureaux centraux nationaux, services nationaux autorisés et entités internationales autorisées, ainsi qu'au Secrétariat général, le niveau de protection à appliquer à leurs informations.

   2. Ces niveaux de confidentialité sont utilisés par le Secrétariat général afin :

      i. d'indiquer aux Bureaux centraux nationaux, services nationaux autorisés et entités internationales autorisées le niveau de protection à appliquer à ses informations ;

      ii. d'attribuer à une information un niveau de confidentialité supérieur à celui indiqué par sa source, en application de l'article 8 (b) du RTI.

c) Si la source d'une information ne lui a attribué aucun niveau de confidentialité, cette information est classée « À USAGE OFFICIEL INTERPOL UNIQUEMENT ».

d) La source d'une information peut à tout moment modifier le niveau de confidentialité qu'elle a attribué à cette information, notamment en lui attribuant un niveau de confidentialité inférieur à celui précédemment indiqué si elle considère que la protection a apporter à l'information peut être moindre. De la même manière, le Secrétariat général, lorsqu'il a attribué à une information un niveau de confidentialité supérieur à celui indiqué par sa source, peut à tout moment modifier ce niveau de confidentialité supérieur.

e) Si un Bureau central national, un service national autorisé ou une entité internationale autorisée a besoin, dans un cas particulier, d'attribuer à certaines informations un niveau de confidentialité plus élevé que ceux indiqués ci-dessus, le Secrétariat général en étudie la possibilité avec la source concernée. Dans l'affirmative, ils concluent un accord spécial définissant les conditions attachées au traitement de ces informations.

Article 20.2 : Conditions attachées à chaque niveau de confidentialité

a) Les informations sont classées :

1. « À USAGE OFFICIEL INTERPOL UNIQUEMENT » si leur divulgation non autorisée est de nature à entraver l'action des services chargés de l'application de la loi ou bien à désavantager ou à discréditer l'Organisation, son personnel, ses membres, les entités autorisées ou les personnes physiques ou morales que lesdites informations concernent ;

2. « DIFFUSION RESTREINTE INTERPOL » si leur divulgation non autorisée est susceptible de compromettre l'action des services chargés de l'application de la loi ou bien de nuire à l'Organisation ou à son personnel, à ses membres, aux entités autorisées ou aux personnes physiques ou morales que lesdites informations concernent ;

3. « CONFIDENTIEL INTERPOL » si leur divulgation non autorisée est susceptible de compromettre gravement l'action des services chargés de l'application de la loi ou bien de nuire gravement à l'Organisation ou à son personnel, à ses membres, aux entités autorisées ou aux personnes physiques ou morales que lesdites informations concernent.

b) Le Secrétariat général élabore et met en œuvre, pour chaque niveau de confidentialité, les procédures d'autorisations ou d'habilitations de sécurité nécessaires aux personnes à qui il confie la responsabilité du traitement des informations au sein du Secrétariat général. À cette fin, et chaque fois qu'il s'agit de leurs ressortissants ou de personnes résidant sur leur territoire, les Bureaux centraux nationaux transmettent au Secrétariat général des informations sur ces personnes, dans la limite des lois existant dans leurs pays respectifs.

c) Les canaux et équipements utilisés aux fins du traitement d'informations sont dotés, selon le niveau de confidentialité attribué à l'information, de dispositifs de sécurité adéquats pour prévenir le risque de divulgation non autorisée.

d) Le Secrétariat général élabore des procédures de traitement administratives que doivent observer, pour chaque niveau de confidentialité, les personnes auxquelles le Secrétariat général a confié la responsabilité du traitement d'informations au sein du Secrétariat général. S'agissant des personnes à qui ils confient la responsabilité du traitement d'informations, il appartient aux Bureaux centraux nationaux et aux entités internationales autorisées d'adopter des procédures de traitement administratives au moins équivalentes à celles du Secrétariat général, de manière à assurer le respect du niveau de confidentialité demandé par la source de l'information.

e) Les personnes auxquelles la responsabilité du traitement d'informations par le canal d'INTERPOL est confiée s'assurent que le niveau de confidentialité attribué à ces informations est respecté. Quand bien même une personne est autorisée à traiter une information, elle ne doit y procéder que dans la mesure où cela est nécessaire par rapport à la finalité recherchée.

CHAPITRE IV

LES DROITS D'ACCÈS ET LES RESTRICTIONS

Article 21 : Disposition générale

Les dispositions de l'article 20 du RTI portant sur l'accès aux informations de police, sont précisées comme suit.

Article 22 : Les droits d'accès

a) Les droits d'accès au système d'information policière sont octroyés à des entités et à des personnes expressément désignées en tenant compte des niveaux de confidentialité définis à l'article 20 du présent Règlement. Ils sont déterminés :

   1. par les Bureaux centraux nationaux pour les entités qu'ils autorisent à consulter et à fournir des informations par le canal d'INTERPOL,

2. par le Secrétariat général pour son personnel et les entités avec lesquelles il a conclu un accord de coopération.

b) En cas de violation par un utilisateur des règles applicables au traitement d'une information de police par le canal d'INTERPOL, le Secrétariat général pourra retirer ou demander au Bureau central national concerné de retirer les droits d'accès octroyés.

c) Les droits d'accès attachés à chaque niveau de confidentialité doivent s'entendre sous réserve des restrictions imposées par la source de l'information ou par le Secrétariat général.

Article 23 : Les restrictions et autres conditions attachées au traitement des informations

a) Les sources des informations doivent indiquer clairement les restrictions et autres conditions de traitement des informations qu'elles communiquent par le réseau d'INTERPOL.

b) Les restrictions à l'accès à une information imposées par sa source s'appliquent à toute forme de demande d'accès à ladite information et peuvent concerner certaines modalités de traitement de l'information.

c) Conformément au RTI, et notamment aux articles 8, 9, 11 (a,3) et 18 (b), le Secrétariat général gère les conditions de traitement d'une information imposées par sa source, ainsi que les restrictions attachées à ladite information de manière à empêcher tout accès interdit, et fait en sorte que toute entité autorisée à accéder à l'information connaisse ces conditions de traitement et ces restrictions, afin qu'elle puisse prendre les mesures qui s'imposent pour les respecter.

CHAPITRE V

L'ACCÈS DIRECT, LE TÉLÉCHARGEMENT ET L'INTERCONNEXION

Article 24 : Disposition générale

Les dispositions des articles du RTI portant sur l'accès direct, le téléchargement et l'interconnexion, visées notamment à l'article 20 du RTI, sont précisées comme suit, conformément aux dispositions de l'article 23 (c,6) dudit RTI.

Article 25 : Définitions

a) Par accès direct, on entend toute opération consistant à obtenir une information par simple interrogation d'une base de données en ligne, sans qu'aucune intervention manuelle sur cette base de données ne soit requise en vue de la fourniture de ladite information.

b) Par téléchargement, on entend toute opération télématique ou informatique consistant à importer des éléments d'une base de données d'une entité dans une base de données d'une autre entité.

c) Par interconnexion, on entend toute liaison électronique des réseaux de communication utilisés par l'Organisation et les entités autorisées visées aux articles 1 (f) et (g) du RTI, consistant à relier leurs bases de données.

Article 26 : Les droits d'accès direct, de téléchargement ou d'interconnexion

a) Le Secrétariat général étudiera avec attention chaque demande d'accès direct, de téléchargement et d'interconnexion reçue des Bureaux centraux nationaux et des entités internationales autorisées.

b) Les droits d'accès direct au système d'information policière, de téléchargement ou d'interconnexion doivent être limités :

1. aux seuls entités utilisateurs désignés susceptibles d'apporter ainsi une aide effective à la coopération policière internationale,
2. aux seules informations nécessaires eu égard à la mission de ces entités autorisées.

c) L'étendue des droits d'accès s'entend sous réserve des restrictions attachées à l'information concernée.

d) En cas de violation des règles liées à l'accès direct, au téléchargement ou à l'interconnexion, le Secrétariat général pourra mettre un terme à l'utilisation de ces procédés de communication.

Article 27 : La gestion des opérations d'accès direct, de téléchargement ou d'interconnexion

a) Dans la mesure du possible, il convient de préférer l'interconnexion au téléchargement.

b) Tout ou partie d'une base de données d'INTERPOL ne peut en principe être téléchargée que dans une seule base de données permanente par pays, déterminée par le B.C.N., ou par entité internationale autorisée.

c) Dans le cas des B.C.N., le Secrétariat général ne peut déroger aux dispositions du point b) ci-dessus qu'aux conditions cumulatives suivantes :

1. cela s'avère indispensable, en raison des caractéristiques fonctionnelles ou techniques d'un pays,
2. le téléchargement reste un processus de traitement utile aux finalités recherchées,
3. les opérations de téléchargement sont soumises à un accord entre le Secrétariat général et le B.C.N. concerné, afin de garantir le respect des règles applicables de l'Organisation.

d) Dans le cas d'une entité internationale autorisée, le Secrétariat général ne peut déroger aux dispositions du point b) ci-dessus que sur la base d'un accord spécifique avec l'entité internationale autorisée, afin de garantir le respect des règles applicables de l'Organisation, l'accord en question ayant été approuvé par l'Assemblée générale.

e) Les dispositions du point b) ci-dessus ne s'appliquent pas quand des données sont téléchargées temporairement d'une base d'INTERPOL pour les comparer avec des données d'une autre base, nationale ou internationale, puis effacées une fois ladite comparaison réalisée.

f) Les restrictions imposées à INTERPOL par les sources des informations s'appliquent *mutatis mutandis* aux utilisateurs desdites informations. Si, pour des raisons techniques ou autres, le Secrétariat général n'est pas en mesure de respecter une restriction associée à une information à télécharger, il ne doit pas autoriser le téléchargement de ladite information.

g) Conformément à l'article 23 ci-dessus, l'entité autorisée, propriétaire de la base dans laquelle sont téléchargées des informations provenant d'une base de données d'INTERPOL, gère les droits d'accès à ladite base en tenant compte des éventuelles restrictions imposées à INTERPOL par les sources des informations, y compris les restrictions relatives à l'accès par des entités tierces ou à la diffusion à de telles entités.

h) Une obligation de transparence et de coopération avec l'Organisation et les sources des informations traitées par le canal d'INTERPOL est associée au droit d'accès direct, de téléchargement ou d'interconnexion. En vertu de cette obligation, le Secrétariat général et la source de l'information doivent être informés :

1. des caractéristiques des bases de données, des équipements ou des réseaux utilisés par les entités autorisées à procéder à ces opérations,
2. de tout élément susceptible de présenter un intérêt concret pour la police au niveau international, au sens de l'article 8 ci-dessus, issu des données obtenues par accès direct, interconnectées ou téléchargés d'une base de données de l'Organisation vers une base de données nationale, et notamment de toute réponse positive générée par lesdites données.

i) Toute entité autorisée par le Secrétariat général à télécharger tout ou partie d'une base de données d'INTERPOL est supposée mettre à jour aussi fréquemment que possible les éléments d'information ainsi téléchargés, y compris lorsque la mise à jour suppose la destruction d'une information ou d'éléments d'information à la demande de la source. Dans tous les cas, la mise à jour doit avoir lieu au moins une fois par semaine.

j) Avant toute utilisation d'une information téléchargée, il convient de vérifier auprès de sa source, voire du Secrétariat général, si elle est exacte et pertinente conformément à l'article 5.5 (a) du RTI.

k) Les informations téléchargées doivent être détruites lorsque la finalité pour laquelle elles ont été téléchargées est atteinte, en particulier lorsque les informations ont été téléchargées en vue de comparaisons.

CHAPITRE VI

LA COOPÉRATION POLICIÈRE AVEC LES ENTITÉS PRIVÉES

Article 28 : Définition de la notion d'« entité privée »

Par « entité privée », on entend toute entité autre que le Secrétariat général, un Bureau central national, une entité nationale autorisée ou une entité internationale autorisée, au sens des articles 1(e) à 1(g) du RTI, et qui a conclu un accord de coopération avec l'Organisation l'autorisant à échanger des informations par le canal de l'Organisation.

Article 29 : Conditions de coopération avec les « entités privées »

a) Toute coopération avec une entité privée doit :

i. respecter le Statut d'INTERPOL et en particulier le principe de souveraineté nationale. De ce fait, conformément à l'article 5.4 du RTI, un B.C.N. source d'une information peut s'opposer à la retransmission de ladite information à une entité privée,

ii. être soumise à des accords, dont la conclusion a préalablement été autorisée par le Comité exécutif puis approuvée par l'Assemblée générale.

b) Une telle coopération ne peut être envisagée que si :

i. la finalité de la coopération est clairement déterminée et correspond à l'une des activités de prévention visées à l'article 3.1 (a,5), (a,8) et (b) du RTI,

ii. elle doit présenter un intérêt concret pour la police au niveau international par rapport à la finalité recherchée,

iii. l'entité privée exerce des activités internationales en rapport avec celles d'INTERPOL et y concourant,

iv. il est envisagé une coopération durable.

c) Les informations fournies aux entités privées devraient être limitées aux informations analytiques et ne devraient pas être à caractère personnel au sens de l'article 1 (c) du RTI.

Néanmoins, les informations fournies aux entités privées peuvent s'étendre, dans le cadre d'un projet spécifique, aux données à caractère personnel (à l'exclusion des données nominatives, sauf si les B.C.N. ou entités internationales autorisées sources l'autorisent expressément) ou aux informations utilisées dans un contexte opérationnel.

Dans ce cas, les conditions supplémentaires suivantes doivent être remplies :

- les limites de projet doivent être clairement définies ;
- le projet doit faire l'objet d'un accord préalable avec les entités concernées ;
- l'utilisation des données doit être proportionnelle aux finalités mentionnées à l'article 3.1 du RTI.

d) Les modalités de communication d'informations aux entités privées autorisées doivent être déterminées de façon à garantir la sécurité, l'intégrité et l'inviolabilité des informations traitées par le canal d'INTERPOL.

Le Secrétariat général devra s'assurer que les moyens utilisés par une entité privée pour fournir ou consulter des informations par le canal d'INTERPOL ne lui permettent d'accéder qu'aux seules informations autorisées, conformément à l'accord conclu à cet effet. Il devra veiller à ce que les entités privées ne puissent ni accéder à des informations opérationnelles, ni compromettre ou interférer avec des communications de police.

e) En aucun cas le canal d'INTERPOL ne peut être utilisé pour contourner les contraintes imposées par toute législation nationale en matière de coopération policière avec une entité privée.

f) L'indépendance de l'Organisation dans sa coopération avec une entité privée doit être garantie. Aucune coopération entre l'Organisation et le secteur privé ne doit interférer avec l'activité principale de l'Organisation, ni l'influencer.

CHAPITRE VII

LE TRAITEMENT DANS TOUT AUTRE BUT LÉGITIME

Article 30 : Disposition générale

Les dispositions des articles 3.2 du RTI, telles que complétées par les dispositions des articles 10.4, 16.2 (a,3), 17.1 (c,3) et 19 (b) dudit RTI portant sur le traitement dans tout autre but légitime sont précisées comme suit, conformément aux dispositions de son article 23 (c,3).

Article 31 : La responsabilité du Secrétariat général

Lorsqu'une information initialement traitée à des fins de coopération policière est ultérieurement traitée dans tout autre but légitime, le Secrétariat général prend les mesures techniques et organisationnelles nécessaires, notamment en matière de sécurité, propres à :

a) assurer le respect des règles de l'Organisation applicables au traitement des informations,

b) et garantir que ce traitement ultérieur n'est pas incompatible avec le traitement initial.

Article 32 : Les modalités générales de traitement

Le traitement dans tout autre but légitime, effectué à l'aide d'informations à caractère personnel enregistrées dans des bases de données d'INTERPOL, doit être motivé.

Article 33 : Les conditions de traitement

a) Le traitement d'informations dans tout autre but légitime doit être limité aux seuls éléments strictement nécessaires aux finalités poursuivies.

b) Le traitement est effectué à l'aide d'informations anonymisées, si possible, et à défaut codées, à chaque fois que la finalité escomptée peut être atteinte par ce procédé.

Article 34 : La communication de l'information

Sous réserve de l'exception visée à l'article 17.1 (c) du RTI, la communication d'une information à caractère personnel traitée dans tout autre but légitime est soumise à l'accord préalable de la source d'information.

Article 35 : La conservation de l'information

Les informations traitées dans tout autre but légitime sont conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées.

CHAPITRE VII

NOTICES

Article 36 : Disposition générale

Aux fins de l'application de l'article 10.5 (c) du RTI, qui concerne les notices, les règles suivantes s'appliquent :

Article 37 : Conditions attachées à l'émission de notices

a) Les notices suivantes peuvent être émises conformément aux buts définis dans l'article 3.1 du RTI et en respectant les conditions spécifiques suivantes :

1. Notices rouges

   i. Les notices rouges sont émises pour demander la localisation et l'arrestation d'une personne en vue de son extradition.

ii. Avant de demander l'émission et la diffusion d'une notice rouge, le Bureau central national ou l'entité internationale autorisée s'assure :
   - que la personne fait l'objet de poursuites pénales ou a été reconnue coupable d'une infraction et que les références d'un mandat d'arrêt, d'une décision de justice ou autre document judiciaire exécutoire sont transmises ;
   - que des assurances ont été données que l'extradition sera demandée lorsque la personne aura été arrêtée, conformément à la législation nationale et/ou aux traités bilatéraux et conventions multilatérales applicables ;
   - que suffisamment d'informations sont fournies pour que la coopération sollicitée soit efficace.

2. Notices bleues

i. Les notices bleues sont émises pour :
   - obtenir des renseignements sur une personne présentant un intérêt au regard d'une enquête criminelle, et/ou
   - localiser une personne présentant un intérêt au regard d'une enquête criminelle, et/ou
   - identifier une personne présentant un intérêt au regard d'une enquête criminelle.

ii. Avant de demander l'émission et la diffusion d'une notice bleue, le Bureau central national, le service national autorisé ou l'entité internationale autorisée s'assure :
   - que la personne concernée présente un intérêt au regard d'une enquête criminelle, par exemple en tant qu'auteur d'une infraction, suspect, complice, associé ou témoin ;
   - que des renseignements complémentaires sur ses éventuels antécédents judiciaires, sur son statut, sur le lieu où elle se trouve, sur son identité ou sur tout autre aspect utile à l'enquête criminelle sont demandés ;
   - que suffisamment d'informations sont fournies pour que la coopération sollicitée soit efficace.

3. Notices vertes

i. Les notices vertes sont émises pour alerter sur les activités criminelles d'une personne.

ii. Avant de demander l'émission et la diffusion d'une notice verte, le Bureau central national, le service national autorisé ou l'entité internationale autorisée s'assure :
   - que la personne est considérée comme constituant une menace pour la sécurité publique et/ou susceptible de commettre une infraction pénale ;

- que cette conclusion se fonde sur une évaluation effectuée par un service national chargé de l'application de la loi ou par une entité internationale autorisée ;
- que cette évaluation se fonde sur l'existence d'une ou de plusieurs condamnations antérieures et/ou sur d'autres motifs raisonnables ;
- que suffisamment d'informations sont fournies pour que la mise en garde soit pertinente.

4. Notices jaunes

   i. Les notices jaunes sont émises pour retrouver une personne disparue ou pour identifier une personne dans l'incapacité de s'identifier elle-même.

   ii. Avant de demander l'émission et la diffusion d'une notice jaune, le Bureau central national, le service national autorisé ou l'entité internationale autorisée s'assure :
   - si la notice est émise pour retrouver une personne disparue, que la disparition a été signalée à la police, que l'on ignore où la personne se trouve et que son anonymat ou sa vie privée n'est pas protégé par la législation nationale applicable ;
   - si la notice est émise pour identifier une personne dans l'incapacité de s'identifier elle-même, que la demande est effectuée parce qu'une personne dans l'incapacité de s'identifier elle-même a été découverte ;
   - que suffisamment d'informations sont fournies pour permettre une identification.

5. Notices noires

   i. Les notices noires sont émises pour identifier des personnes décédées.

   ii. Avant de demander l'émission et la diffusion d'une notice noire, le Bureau central national, le service national autorisé ou l'entité internationale autorisée s'assure :
   - que la demande est effectuée parce qu'un cadavre a été découvert qui n'a pu être identifié ;
   - que suffisamment d'informations sont fournies pour permettre une identification.

6. Œuvres d'art volées

   i. Les notices relatives aux œuvres d'art volées sont émises pour localiser des œuvres d'art ou des objets ayant une valeur culturelle qui ont été volés, ou pour identifier de tels objets découverts dans des circonstances suspectes.

ii. Avant de demander l'émission et la diffusion d'une notice relative à une œuvre d'art volée, le Bureau central national, le service national autorisé ou l'entité internationale autorisée s'assure :
   - que l'œuvre d'art, ou l'objet ayant une valeur culturelle présente un intérêt au regard d'une enquête criminelle ;
   - qu'il présente un caractère unique et/ou a une valeur commerciale importante ;
   - que suffisamment d'informations sont fournies pour permettre une identification.

7. Notices mauves
   i. Les notices mauves sont émises pour fournir des informations sur un mode opératoire, des procédés, des objets, des équipements et des caches utilisés par les criminels ;
   ii. Avant de demander l'émission et la diffusion d'une notice mauve, le Bureau central national, le service national autorisé ou l'entité internationale autorisée s'assure que la diffusion des informations sous la forme d'une notice présente un intérêt concret pour la police au niveau international et est dans l'intérêt de la sécurité publique.

8. Notices spéciales
   i. Les notices spéciales sont émises en vertu d'un accord conclu avec une autre organisation internationale en application de l'article 41 du Statut.
   ii. Avant de demander l'émission et la diffusion d'une notice spéciale, l'entité internationale autorisée s'assure :
      - que les informations remplissent les conditions nécessaires à l'émission de notices de ce type, telles que précisées dans ledit accord ;
      - que suffisamment d'informations sont fournies pour que la coopération sollicitée soit efficace.

9. Notices orange
   i. Les notices orange sont émises pour alerter sur un événement, une personne, un objet, un procédé ou un mode opératoire constituant une menace imminente pour la sécurité publique et susceptible de porter gravement atteinte aux personnes et/ou aux biens.

ii. Avant de demander l'émission et la diffusion d'une notice orange, le Bureau central national, le service national autorisé ou l'entité internationale autorisée s'assure :
   - dans le cas d'une personne, qu'elle est considérée comme constituant une menace imminente pour la sécurité publique et/ou susceptible de commettre une infraction pénale ; cette conclusion se fonde sur une évaluation effectuée par un service national chargé de l'application de la loi ; cette évaluation se fonde sur l'existence d'une ou de plusieurs condamnations antérieures et/ou sur d'autres motifs raisonnables ;
   - dans le cas d'un objet, d'un événement ou d'un mode opératoire, qu'il est considéré comme constituant une menace imminente pour la sécurité publique ; cette conclusion se fonde sur une évaluation effectuée par un service national chargé de l'application de la loi ;
   - que suffisamment d'informations sont fournies pour que la mise en garde soit pertinente.

iii. Les notices orange constituent des alertes et il appartient à chaque pays de prendre les dispositions adéquates, conformément à la législation nationale applicable.

b) Avant d'émettre et de diffuser une notice de sa propre initiative, le Secrétariat général s'assure que les conditions attachées à la notice en question sont remplies.

c) Le Secrétaire Général peut créer tout autre type de notice qu'il juge nécessaire pour aider l'Organisation à s'acquitter de son mandat conformément à son Statut, au RTI et au présent Règlement d'application. Il rend compte de cette création à l'Assemblée générale.

Article 38 : Modalités de traitement des notices

a) Le Secrétariat général définit et modifie, s'il y a lieu, le type d'informations devant figurer dans les demandes de notices, sous réserve de respecter les conditions attachées aux notices en question, ainsi que toutes autres directives ou décisions émanant de l'Assemblée générale ou du Comité exécutif.

b) Le Secrétariat général ne peut émettre une notice qu'après avoir contrôlé la conformité du traitement requis aux règles en vigueur et que si le Bureau central national, le service national autorisé ou l'entité internationale autorisée ayant demandé l'émission lui a communiqué tous les ensembles d'informations requis.

c) Avant d'émettre une notice à la demande d'un Bureau central national, d'un service national autorisé ou d'une entité internationale autorisée, et chaque fois qu'il découvre des ensembles d'informations enregistrés dans le système d'information policière susceptibles de revêtir de l'importance au regard de l'émission de ladite notice, le Secrétariat général, sous réserve de toute restriction imposée par la source de l'information, et en accord avec l'entité ayant demandé l'émission de la notice, détermine s'il convient d'inclure ou non les ensembles d'informations concernés dans la notice. S'il inclut ces ensembles d'informations dans la notice, le Secrétariat général attribue par ailleurs ce complément d'informations à l'entité qui en est la source.

d) Lorsque la menace ayant justifié l'émission d'une notice orange ne revêt plus un caractère imminent, le Secrétariat général, en consultation avec le Bureau central national, le service national autorisé ou l'entité internationale autorisée ayant demandé son émission, peut procéder à son remplacement par toute autre notice appropriée.

e) Avant d'émettre une notice de sa propre initiative, le Secrétariat général s'assure que les sources des ensembles d'informations enregistrés dans le système d'information policière et dont le Secrétariat général a établi qu'ils revêtent une importance au regard de l'émission de ladite notice ont autorisé leur publication dans une notice.

f) La divulgation au public d'une notice et de tout ou partie de l'information contenue dans celle-ci est soumise :

   1. à l'autorisation préalable de la source de l'information, et
   2. à l'acceptation par le Secrétariat général de procéder à cette divulgation, étant entendu que le Secrétariat général détermine les ensembles d'informations contenus dans la notice qui peuvent être divulgués au public.

g) D'autres méthodes que celles décrites ci-dessus peuvent être utilisées pour traiter les notices spéciales émises en vertu d'un accord conclu avec une autre organisation internationale en application de l'article 41 du Statut.

CHAPITRE IX

CONFORMITÉ AU STATUT ET AUX RÈGLES DE L'ORGANISATION APPLICABLES EN LA MATIÈRE

Article 39 : Disposition générale

Aux fins de l'application de l'article 10.1 (a,1) du RTI, qui concerne la conformité au Statut d'INTERPOL et aux règles de l'Organisation applicables en la matière comme condition au traitement d'informations, les règles suivantes s'appliquent.

Article 40 : Article 3 du Statut d'INTERPOL

a) Pour déterminer si une activité ou intervention dans des questions ou affaires présente un caractère politique, militaire, religieux ou racial, toutes les informations pertinentes sont examinées, notamment :

   i. la nature de l'infraction, à savoir les chefs d'accusation et les faits concernés ;

   ii. le statut des personnes concernées ;

   iii. l'identité de la source des informations ;

   iv. la position exprimée par un Membre ou une entité internationale autorisée autre que la source des informations ;

   v. les obligations de droit international ;

   vi. les implications au regard de la neutralité de l'Organisation ;

   vii. le contexte général de l'affaire.

b) Les Bureaux centraux nationaux et les entités internationales autorisées informent dès que possible le Secrétariat général s'il existe un doute concernant le respect de l'article 3 du Statut par le traitement d'une information.

c) Le Secrétariat général élabore un recueil de pratiques sur l'application de l'article 3 du Statut à partir des directives émanant de l'Assemblée générale et des éléments pertinents du droit international. Ce recueil est mis à la disposition des Bureaux centraux nationaux, des services nationaux autorisés et des entités internationales autorisées.

- - - - - - -